Network Working Group
Request for Comments: 2548
Category: Informational
G. Zorn
Microsoft Corporation
March 1999

Microsoft Vendor-specific RADIUS Attributes

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This document describes the set of Microsoft vendor-specific RADIUS attributes. These attributes are designed to support Microsoft proprietary dial-up protocols and/or provide support for features which is not provided by the standard RADIUS attribute set [3]. It is expected that this memo will be updated whenever Microsoft defines a new vendor-specific attribute, since its primary purpose is to provide an open, easily accessible reference for third-parties wishing to interoperate with Microsoft products.

1. Specification of Requirements

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT" are to be interpreted as described in [2].

2. Attributes

The following sections describe sub-attributes which may be transmitted in one or more RADIUS attributes of type Vendor-Specific [3]. More than one sub-attribute MAY be transmitted in a single Vendor-Specific Attribute; if this is done, the sub-attributes SHOULD be packed as a sequence of Vendor-Type/Vendor-Length/Value triples following the inital Type, Length and Vendor-ID fields. The Length field of the Vendor-Specific Attribute MUST be set equal to the sum of the Vendor-Length fields of the sub-attributes contained in the Vendor-Specific Attribute, plus six. The Vendor-ID field of the Vendor-Specific Attribute(s) MUST be set to decimal 311 (Microsoft).

2.1. Attributes for Support of MS-CHAP Version 1

2.1.1. Introduction

Microsoft created Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) [4] to authenticate remote Windows workstations, providing the functionality to which LAN-based users are accustomed. Where possible, MS-CHAP is consistent with standard CHAP [5], and the differences are easily modularized. Briefly, the differences between MS-CHAP and standard CHAP are:

* MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.

* The MS-CHAP Response packet is in a format designed for compatibility with Microsoft Windows NT 3.5, 3.51 and 4.0, Microsoft Windows95, and Microsoft LAN Manager 2.x networking products. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.

* MS-CHAP provides an authenticator-controlled authentication retry mechanism.

* MS-CHAP provides an authenticator-controlled password changing mechanism.

* MS-CHAP defines an extended set of reason-for-failure codes, returned in the Failure packet Message field.

The attributes defined in this section reflect these differences.

2.1.2. MS-CHAP-Challenge

Description

This Attribute contains the challenge sent by a NAS to a Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user. It MAY be used in both Access-Request and Access-Challenge packets.

A summary of the MS-CHAP-Challenge Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
11 for MS-CHAP-Challenge.

Vendor-Length
> 2

String
The String field contains the MS-CHAP challenge.

2.1.3. MS-CHAP-Response

Description

This Attribute contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge. It is only used in Access-Request packets.

A summary of the MS-CHAP-Response Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Ident     |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            LM-Response
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         LM-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         LM-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         LM-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         LM-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         LM-Response(cont)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           NT-Response
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         NT-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         NT-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         NT-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         NT-Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         NT-Response (cont)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   1 for MS-CHAP-Response.

Vendor-Length
   52

Ident
   Identical to the PPP CHAP Identifier.

Flags
   The Flags field is one octet in length. If the Flags field is one (0x01), the NT-Response field is to be used in preference to the LM-Response field for authentication. The LM-Response field MAY still be used (if non-empty), but the NT-Response SHOULD be tried first. If it is zero, the NT-Response field MUST be ignored and the LM-Response field used.

LM-Response

The LM-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

NT-Response

The NT-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

2.1.4. MS-CHAP-Domain

Description

The MS-CHAP-Domain Attribute indicates the Windows NT domain in which the user was authenticated. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-CHAP-Domain Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Ident     |    String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type

10 for MS-CHAP-Domain.

Vendor-Length

> 3

Ident

The Ident field is one octet and aids in matching requests and replies.

String

This field contains the name in ASCII of the Windows NT domain in which the user was authenticated.

2.1.5. MS-CHAP-Error

Description

The MS-CHAP-Error Attribute contains error data related to the preceding MS-CHAP exchange. This Attribute may be used in both MS-CHAP-V1 and MS-CHAP-V2 (see below) exchanges. It is only used in Access-Reject packets.

A summary of the MS-CHAP-Error Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Ident     |    String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   2 for MS-CHAP-Error.

Vendor-Length
   > 3

Ident
   The Ident field is one octet and aids in matching requests and replies.

String
   This field contains specially formatted ASCII text, which is interpreted by the authenticating peer.

2.1.6. MS-CHAP-CPW-1

Description

This Attribute allows the user to change their password if it has expired. This Attribute is only used in Access-Request packets, and should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is less than 2.

A summary of the MS-CHAP-CPW-1 Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Code      |     Ident     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        LM-Old-Password
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-Old-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-Old-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-Old-Password (cont)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        LM-New-Password
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-New-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-New-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      LM-New-Password (cont)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        NT-Old-Password
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-Old-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-Old-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-Old-Password (cont)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        NT-New-Password
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-New-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-New-Password (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                      NT-New-Password (cont)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     New-LM-Password-Length    |             Flags             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   3 for MS-CHAP-PW-1

Vendor-Length
   72

Code
   The Code field is one octet in length. Its value is always 5.

Ident
The Ident field is one octet and aids in matching requests and replies.

LM-Old-Password
The LM-Old-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the old password.

LM-New-Password
The LM-New-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the new password.

NT-Old-Password
The NT-Old-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the old password.

NT-New-Password
The NT-New-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the new password.

New-LM-Password-Length
The New-LM-Password-Length field is two octets in length and contains the length in octets of the new LAN Manager-compatible password.

Flags
The Flags field is two octets in length. If the least significant bit of the Flags field is one, this indicates that the NT-New-Password and NT-Old-Password fields are valid and SHOULD be used. Otherwise, the LM-New-Password and LM-Old-Password fields MUST be used.

2.1.7. MS-CHAP-CPW-2

Description

This Attribute allows the user to change their password if it has expired. This Attribute is only used in Access-Request packets, and should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is equal to 2.

A summary of the MS-CHAP-CPW-2 Attribute format is shown below. The fields are transmitted from left to right.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-Type  | Vendor-Length |     Code      |     Ident     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Old-NT-Hash
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-NT-Hash (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-NT-Hash (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-NT-Hash (cont)                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Old-LM-Hash
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-LM-Hash(cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-LM-Hash(cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Old-LM-Hash(cont)                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         LM-Response
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Response (cont)                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          NT-Response
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--++-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--++-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             Flags             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type

4 for MS-CHAP-PW-2

Vendor-Length

86

Code

6

Ident

The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical to that in the Ident field in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes contained in a single Access-Request packet.

Old-NT-Hash

The Old-NT-Hash field is 16 octets in length. It contains the old Windows NT password hash encrypted with the new Windows NT password hash.

Old-LM-Hash

The Old-LM-Hash field is 16 octets in length. It contains the old Lan Manager password hash encrypted with the new Windows NT password hash.

LM-Response

The LM-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

NT-Response

The NT-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

Flags

The Flags field is two octets in length. If the least significant bit (bit 0) of this field is one, the NT-Response field is to be used in preference to the LM-Response field for authentication. The LM-Response field MAY still be used (if present), but the NT-Response SHOULD be tried first. If least significant bit of the field is zero, the NT-Response field MUST be ignored and the LM-Response field used instead. If bit 1 of the Flags field is one, the Old-LM-Hash field is valid and SHOULD be used. If this bit is set, at least one instance of the MS-CHAP-LM-Enc-PW attribute MUST be included in the packet.

2.1.8. MS-CHAP-LM-Enc-PW

Description

This Attribute contains the new Windows NT password encrypted with the old LAN Manager password hash. The encrypted Windows NT password is 516 octets in length; since this is longer than the maximum lengtth of a RADIUS attribute, the password must be split into several attibutes for transmission. A 2 octet sequence number is included in the attribute to help preserve ordering of the password fragments.

This Attribute is only used in Access-Request packets, in conjunction with the MS-CHAP-CPW-2 attribute. It should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is 2 or greater.

A summary of the MS-CHAP-LM-Enc-PW Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |      Code     |     Ident     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Sequence-Number         |          String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   5 for MS-CHAP-LM-Enc-PW

Vendor-Length
   > 6

Code 6. Code is the same as for the MS-CHAP-PW-2 attribute.

Ident
   The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes which are present in the same Access-Request packet.

Sequence-Number
The Sequence-Number field is two octets in length and indicates which "chunk" of the encrypted password is contained in the following String field.

String The String field contains a portion of the encrypted password.

2.2. MS-CHAP-NT-Enc-PW

Description

This Attribute contains the new Windows NT password encrypted with the old Windows NT password hash. The encrypted Windows NT password is 516 octets in length; since this is longer than the maximum lengtth of a RADIUS attribute, the password must be split into several attibutes for transmission. A 2 octet sequence number is included in the attribute to help preserve ordering of the password fragments.

This Attribute is only used in Access-Request packets, in conjunction with the MS-CHAP-CPW-2 and MS-CHAP2-CPW attributes. It should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is 2 or greater.

A summary of the MS-CHAP-NT-Enc-PW Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |      Code     |     Ident     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Sequence-Number       |           String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
6 for MS-CHAP-NT-Enc-PW

Vendor-Length
> 6

Code
6. Code is the same as for the MS-CHAP-PW-2 attribute.

Ident

The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes which are present in the same Access-Request packet.

Sequence-Number

The Sequence-Number field is two octets in length and indicates which "chunk" of the encrypted password is contained in the following String field.

String

The String field contains a portion of the encrypted password.

2.3. Attributes for Support of MS-CHAP Version 2

2.3.1. Introduction

This section describes RADIUS attributes supporting version two of Microsoft’s PPP CHAP dialect (MS-CHAP-V2) [14]. MS-CHAP-V2 is similar to, but incompatible with, MS-CHAP version one (MS-CHAP-V1) [4]. Certain protocol fields have been deleted or reused but with different semantics. Where possible, MS-CHAP-V2 is consistent with both MS-CHAP-V1 and standard CHAP [1]. Briefly, the differences between MS-CHAP-V2 and MS-CHAP-V1 are:

* MS-CHAP-V2 is enabled by negotiating CHAP Algorithm 0x81 in LCP option 3, Authentication Protocol.

* MS-CHAP-V2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

* The calculation of the "Windows NT compatible challenge response" sub-field in the Response packet has been changed to include the peer challenge and the user name.

* In MS-CHAP-V1, the "LAN Manager compatible challenge response" sub-field was always sent in the Response packet. This field has been replaced in MS-CHAP-V2 by the Peer-Challenge field.

* The format of the Message field in the Failure packet has been changed.

* The Change Password (version 1) and Change Password (version 2) packets are no longer supported. They have been replaced with a single Change-Password packet.

The attributes defined in this section reflect these differences.

2.3.2. MS-CHAP2-Response

Description

This Attribute contains the response value provided by an MS-CHAP-V2 peer in response to the challenge. It is only used in Access-Request packets.

A summary of the MS-CHAP2-Response Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Ident     |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Peer-Challenge
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         Peer-Challenge (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         Peer-Challenge (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         Peer-Challenge (cont)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Reserved
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Reserved (cont)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Response
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Response (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            Response (cont)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   25 for MS-CHAP2-Response.

Vendor-Length
   52

Ident
Identical to the PPP MS-CHAP v2 Identifier.

Flags
The Flags field is one octet in length. It is reserved for future use and MUST be zero.

Peer-Challenge
The Peer-Challenge field is a 16-octet random number.

Reserved
This field is reserved for future use and MUST be zero.

Response
The Response field is 24 octets in length and holds an encoded function of the password, the Peer-Challenge field and the received challenge.

2.3.3. MS-CHAP2-Success

Description

This Attribute contains a 42-octet authenticator response string. This string MUST be included in the Message field of the MS-CHAP-V2 Success packet sent from the NAS to the peer. This Attribute is only used in Access-Accept packets.

A summary of the MS-CHAP2-Success Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |     Ident     |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
26 for MS-CHAP2-Success.

Vendor-Length
45

Ident
Identical to the PPP MS-CHAP v2 Identifier.

String
The 42-octet authenticator string (see above).

2.3.4. MS-CHAP2-CPW

Description

This Attribute allows the user to change their password if it has expired. This Attribute is only used in conjunction with the MS-CHAP-NT-Enc-PW attribute in Access-Request packets, and should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is equal to 3.

A summary of the MS-CHAP-CPW-2 Attribute format is shown below. The fields are transmitted from left to right.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-Type  | Vendor-Length |     Code      |     Ident     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Encrypted-Hash
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Encrypted-Hash (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Encrypted-Hash (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Encrypted-Hash (cont)                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Peer-Challenge
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Peer-Challenge (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Peer-Challenge (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Peer-Challenge (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Peer-Challenge (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Peer-Challenge (cont)                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          NT-Response
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--++-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--++-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Response (cont)                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             Flags             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   27 for MS-CHAP2-PW

Vendor-Length
   70

Code
   7

Ident

The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical to that in the Ident field in all instances of the MS-CHAP-NT-Enc-PW contained in the Access-Request packet.

Encrypted-Hash

The Encrypted-Hash field is 16 octets in length. It contains the old Windows NT password hash encrypted with the new Windows NT password hash.

NT-Response

The NT-Response field is 24 octets in length and holds an encoded function of the new password, the Peer-Challenge field and the received challenge.

Flags

The Flags field is two octets in length. This field is reserved for future use and MUST be zero.

2.4. Attributes for MPPE Support

This section describes a set of Attributes designed to support the use of Microsoft Point-to-Point Encryption (MPPE) [6] in dial-up networks. MPPE is a means of representing Point to Point Protocol (PPP) [7] packets in a encrypted form. MPPE uses the RSA RC4 [8] algorithm for encryption. The length of the session key to be used for initializing encryption tables can be negotiated; MPPE currently supports 40 bit and 128 bit session keys. MPPE is negotiated within option 18 in the PPP Compression Control Protocol (CCP)[9], [10].

2.4.1. MS-CHAP-MPPE-Keys

Description

The MS-CHAP-MPPE-Keys Attribute contains two session keys for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This Attribute is only included in Access-Accept packets.

A summary of the MS-CHAP-MPPE-Keys Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           Keys
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           Keys (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Keys (cont)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   12 for MS-CHAP-MPPE-Keys.

Vendor-Length
   34

Keys
   The Keys field consists of two logical sub-fields: the LM-Key and the NT-Key. The LM-Key is eight octets in length and contains the first eight bytes of the output of the function LmPasswordHash(P, This hash is constructed as follows: let the plain-text password be represented by P.

   The NT-Key sub-field is sixteen octets in length and contains the first sixteen octets of the hashed Windows NT password. The format of the plaintext Keys field is illustrated in the following diagram:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             LM-Key
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           LM-Key (cont)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             NT-Key
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Key (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Key (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                           NT-Key (cont)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Padding
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          Padding (cont)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Keys field MUST be encrypted by the RADIUS server using the same method defined for the User-Password Attribute [3]. Padding is required because the method referenced above requires the field to be encrypted to be a multiple of sixteen octets in length.

Implementation Note

This attribute should only be returned in response to an Access-Request packet containing MS-CHAP attributes.

2.4.2. MS-MPPE-Send-Key

Description

The MS-MPPE-Send-Key Attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). As the name implies, this key is intended for encrypting packets sent from the NAS to the remote host. This Attribute is only included in Access-Accept packets.

A summary of the MS-MPPE-Send-Key Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Salt
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
16 for MS-MPPE-Send-Key.

Vendor-Length
> 4

Salt
The Salt field is two octets in length and is used to ensure the uniqueness of the keys used to encrypt each of the encrypted attributes occurring in a given Access-Accept packet. The most significant bit (leftmost) of the Salt field MUST be set (1). The contents of each Salt field in a given Access-Accept packet MUST be unique.

String
The plaintext String field consists of three logical sub-fields: the Key-Length and Key sub-fields (both of which are required), and the optional Padding sub-field. The Key-Length sub-field is one octet in length and contains the length of the unencrypted Key sub-field. The Key sub-field contains the actual encryption key. If the combined length (in octets) of the unencrypted Key-Length and Key sub-fields is not an even multiple of 16, then the Padding sub-field MUST be present. If it is present, the length of the Padding sub-field is variable, between 1 and 15 octets. The String field MUST be encrypted as follows, prior to transmission:

Construct a plaintext version of the String field by concatenating the Key-Length and Key sub-fields. If necessary, pad the resulting string until its length (in octets) is an even multiple of 16. It is recommended that zero octets (0x00) be used for padding. Call this plaintext P.

Call the shared secret S, the pseudo-random 128-bit Request Authenticator (from the corresponding Access-Request packet) R, and the contents of the Salt field A. Break P into 16 octet chunks p(1), p(2)...p(i), where i = len(P)/16. Call the ciphertext blocks c(1), c(2)...c(i) and the final ciphertext C. Intermediate values b(1), b(2)...c(i) are required. Encryption is performed in the following manner (’+’ indicates concatenation):

```
b(1) = MD5(S + R + A)    c(1) = p(1) xor b(1)   C = c(1)
b(2) = MD5(S + c(1))     c(2) = p(2) xor b(2)   C = C + c(2)
            .                      .
            .                      .
            .                      .
b(i) = MD5(S + c(i-1))   c(i) = p(i) xor b(i)   C = C + c(i)
```

The resulting encrypted String field will contain c(1)+c(2)+...+c(i).

On receipt, the process is reversed to yield the plaintext String.

Implementation Notes

It is possible that the length of the key returned may be larger than needed for the encryption scheme in use. In this case, the RADIUS client is responsible for performing any necessary truncation.

This attribute MAY be used to pass a key from an external (e.g., EAP [15]) server to the RADIUS server. In this case, it may be impossible for the external server to correctly encrypt the key, since the RADIUS shared secret might be unavailable. The external server SHOULD, however, return the attribute as defined above; the Salt field SHOULD be zero-filled and padding of the String field SHOULD be done. When the RADIUS server receives the attribute from the external server, it MUST correctly set the Salt field and encrypt the String field before transmitting it to the RADIUS client. If the channel used to communicate the MS-MPPE-Send-Key attribute is not secure from eavesdropping, the attribute MUST be cryptographically protected.

2.4.3. MS-MPPE-Recv-Key

Description

The MS-MPPE-Recv-Key Attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). As the name implies, this key is intended for encrypting packets received by the NAS from the remote host. This Attribute is only included in Access-Accept packets.

A summary of the MS-MPPE-Recv-Key Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Salt
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type

17 for MS-MPPE-Recv-Key.

Vendor-Length

> 4

Salt

The Salt field is two octets in length and is used to ensure the uniqueness of the keys used to encrypt each of the encrypted attributes occurring in a given Access-Accept packet. The most significant bit (leftmost) of the Salt field MUST be set (1). The contents of each Salt field in a given Access-Accept packet MUST be unique.

String

The plaintext String field consists of three logical sub-fields: the Key-Length and Key sub-fields (both of which are required), and the optional Padding sub-field. The Key-Length sub-field is one octet in length and contains the length of the unencrypted Key sub-field. The Key sub-field contains the actual encryption key. If the combined length (in octets) of the unencrypted Key-Length and Key sub-fields is not an even multiple of 16, then the Padding sub-field MUST be present. If it is present, the length of the Padding sub-field is variable, between 1 and 15 octets. The String field MUST be encrypted as follows, prior to transmission:

Construct a plaintext version of the String field by concatenating the Key-Length and Key sub-fields. If necessary, pad the resulting string until its length (in octets) is an even multiple of 16. It is recommended that zero octets (0x00) be used for padding. Call this plaintext P.

Call the shared secret S, the pseudo-random 128-bit Request Authenticator (from the corresponding Access-Request packet) R, and the contents of the Salt field A. Break P into 16 octet chunks p(1), p(2)...p(i), where i = len(P)/16. Call the ciphertext blocks c(1), c(2)...c(i) and the final ciphertext C. Intermediate values b(1), b(2)...c(i) are required. Encryption is performed in the following manner ('+' indicates concatenation):

```
b(1) = MD5(S + R + A)    c(1) = p(1) xor b(1)   C = c(1)
b(2) = MD5(S + c(1))     c(2) = p(2) xor b(2)   C = C + c(2)
            .                       .
            .                       .
            .                       .
b(i) = MD5(S + c(i-1))   c(i) = p(i) xor b(i)   C = C + c(i)
```

The resulting encrypted String field will contain c(1)+c(2)+...+c(i).

On receipt, the process is reversed to yield the plaintext String.

Implementation Notes

It is possible that the length of the key returned may be larger than needed for the encryption scheme in use. In this case, the RADIUS client is responsible for performing any necessary truncation.

This attribute MAY be used to pass a key from an external (e.g., EAP [15]) server to the RADIUS server. In this case, it may be impossible for the external server to correctly encrypt the key, since the RADIUS shared secret might be unavailable. The external server SHOULD, however, return the attribute as defined above; the Salt field SHOULD be zero-filled and padding of the String field SHOULD be done. When the RADIUS server receives the attribute from the external server, it MUST correctly set the Salt field and encrypt the String field before transmitting it to the RADIUS client. If the channel used to communicate the MS-MPPE-Recv-Key attribute is not secure from eavesdropping, the attribute MUST be cryptographically protected.

2.4.4. MS-MPPE-Encryption-Policy

Description

The MS-MPPE-Encryption-Policy Attribute may be used to signify whether the use of encryption is allowed or required. If the Policy field is equal to 1 (Encryption-Allowed), any or none of the encryption types specified in the MS-MPPE-Encryption-Types Attribute MAY be used. If the Policy field is equal to 2 (Encryption-Required), any of the encryption types specified in the MS-MPPE-Encryption-Types Attribute MAY be used, but at least one MUST be used.

A summary of the MS-MPPE-Encryption-Policy Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Policy
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Policy (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   7 for MS-MPPE-Encryption-Policy.

Vendor-Length
   6

Policy
   The Policy field is 4 octets in length. Defined values are:

      1   Encryption-Allowed 2   Encryption-Required

2.4.5. MS-MPPE-Encryption-Types

Description

The MS-MPPE-Encryption-Types Attribute is used to signify the types of encryption available for use with MPPE. It is a four octet integer that is interpreted as a string of bits.

A summary of the MS-MPPE-Encryption-Policy Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Types
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            Types (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   8 for MS-MPPE-Encryption-Types.

Vendor-Length
   6

Policy
   The Types field is 4 octets in length. The following diagram illustrates the Types field.

```
   3                   2                   1
 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                         |S|L| |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

If the L bit is set, RC4[5] encryption using a 40-bit key is allowed. If the S bit is set, RC4 encryption using a 128-bit key is allowed. If both the L and S bits are set, then either 40- or 128-bit keys may be used with the RC4 algorithm.

2.5. Attributes for BAP Support

This section describes a set of vendor-specific RADIUS attributes designed to support the dynamic control of bandwidth allocation in multilink PPP [11]. Attributes are defined that specify whether use of the PPP Bandwidth Allocation Protocol (BAP) [12] is allowed or required on incoming calls, the level of line capacity (expressed as a percentage) below which utilization must fall before a link is eligible to be dropped, and the length of time (in seconds) that a link must be under-utilized before it is dropped.

2.5.1. MS-BAP-Usage

Description

This Attribute describes whether the use of BAP is allowed, disallowed or required on new multilink calls. It MAY be used in Access-Accept packets.

A summary of the MS-BAP-Usage Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |            Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   13 for MS-BAP-Usage.

Vendor-Length
   6

Value
The Value field is four octets.

```
0      BAP usage not allowed
1      BAP usage allowed
2      BAP usage required
```

2.5.2. MS-Link-Utilization-Threshold

Description

This Attribute represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination. Permissible values for the MS-Link-Utilization-Threshold Attribute are in the range 1-100, inclusive. It is only used in Access-Accept packets.

A summary of the MS-Link-Utilization-Threshold Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |            Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
14 for MS-Link-Utilization-Threshold

Vendor-Length 6

Value The Value field is four octets in length and represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination. Permissible values are in the range 1-100, inclusive.

2.5.3. MS-Link-Drop-Time-Limit

Description

The MS-Link-Drop-Time-Limit Attribute indicates the length of time (in seconds) that a link must be underutilized before it is dropped. It MAY only be included in Access-Accept packets.

A summary of the MS-Link-Drop-Time-Limit Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          Value (cont)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   15 for MS-Link-Drop-Time-Limit

Vendor-Length
   6

Value
   The Value field represents the number of seconds that a link must be underutilized (i.e., display bandwidth utilization below the threshold specified in the MS-Link-Utilization-Threshold Attribute) before the link is dropped.

2.6. Attributes for ARAP Support

This section describes a set of Attributes designed to support the Apple Remote Access Protocol (ARAP).

2.6.1. MS-Old-ARAP-Password

Description

The MS-Old-ARAP-Password Attribute is used to transmit the old ARAP password during an ARAP password change operation. It MAY be included in Access-Request packets.

A summary of the MS-Old-ARAP-Password Attribute Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   19 for MS-Old-ARAP-Password Attribute

Vendor-Length
   > 3

String
The String field is one or more octets. It contains the old ARAP password DES-encrypted using itself as the key.

2.6.2. MS-New-ARAP-Password

Description

The MS-New-ARAP-Password Attribute is used to transmit the new ARAP password during an ARAP password change operation. It MAY be included in Access-Request packets.

A summary of the MS-New-ARAP-Password Attribute Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
20 for MS-New-ARAP-Password Attribute

Vendor-Length
> 3

String
The String field is one or more octets. It contains the new ARAP password DES-encrypted using the old ARAP password as the key.

2.6.3. MS-ARAP-Password-Change-Reason

Description

The MS-ARAP-Password-Change-Reason Attribute is used to indicate reason for a server-initiated password change. It MAY be included in Access-Challenge packets.

A summary of the MS-ARAP-Password-Change-Reason Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |             Why
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            Why (cont)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   21 for MS-ARAP-Password-Change-Reason

Vendor-Length
   6

Why
   The Why field is 4 octets in length. The following values are
   defined:

```
      Just-Change-Password            1
      Expired-Password                2
      Admin-Requires-Password-Change  3
      Password-Too-Short              4
```

2.6.4. MS-ARAP-Challenge

Description

   This attribute is only present in an Access-Request packet
   containing a Framed-Protocol Attribute with the value 3 (ARAP).

A summary of the MS-ARAP-Challenge Attribute format is given below.
The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           Challenge
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                         Challenge (cont)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Challenge (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   33 for MS-ARAP-Challenge

Vendor-Length
   10

Value
The Challenge Field is 8 octets in length. It contains the challenge (as two 4-octet quantities) sent by the NAS to the peer.

2.7. Miscellaneous Attributes

This section describes attributes which do not fall into any particular category, but are used in the identification and operation of Microsoft remote access products.

2.7.1. MS-RAS-Vendor

Description

The MS-RAS-Vendor Attribute is used to indicate the manufacturer of the RADIUS client machine. It MAY be included in both Access-Request and Accounting-Request packets.

A summary of the MS-RAS-Vendor Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           Vendor-ID
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Vendor-ID (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
9 for MS-RAS-Vendor

Vendor-Length
6

Vendor-ID
The Vendor-ID field is 4 octets in length. The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers RFC [13].

2.7.2. MS-RAS-Version

Description

The MS-RAS-Version Attribute is used to indicate the version of the RADIUS client software. This attribute SHOULD be included in packets containing an MS-RAS-Vendor Attribute; it SHOULD NOT be

sent in packets which do not contain an MS-RAS-Vendor Attribute. It MAY be included in both Access-Request and Accounting-Request packets.

A summary of the MS-RAS-Version Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   18 for MS-RAS-Version

Vendor-Length
   > 3

String
   The String field is one or more octets. The actual format of the information is vendor specific, and a robust implementation SHOULD support the field as undistinguished octets.

2.7.3. MS-Filter

Description

The MS-Filter Attribute is used to transmit traffic filters. It MAY be included in both Access-Accept and Accounting-Request packets.

If multiple MS-Filter Attributes are contained within a packet, they MUST be in order and they MUST be consecutive attributes in the packet.

A summary of the MS-Filter Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           Filter...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   22 for MS-Filter Attribute

Vendor-Length
   > 3

Filter
   The Filter field is one or more octets. It contains a sequence of undifferentiated octets.

   If multiple MS-Filter Attributes occur in a single Access-Accept packet, the Filter field from each MUST be concatenated in the order received to form the actual filter.

2.7.4. MS-Acct-Auth-Type

Description

   The MS-Acct-Auth-Type Attribute is used to represent the method used to authenticate the dial-up user. It MAY be included in Accounting-Request packets.

A summary of the MS-Acct-Auth-Type Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           Auth-Type
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         Auth-Type (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   23 for MS-Acct-Auth-Type

Vendor-Length
   6

Auth-Type
   The Auth-Type field is 4 octets in length. The following values are defined for this field:

```
PAP                 1
CHAP                2
MS-CHAP-1           3
MS-CHAP-2           4
EAP                 5
```

2.7.5. MS-Acct-EAP-Type

Description

The MS-Acct-EAP-Type Attribute is used to represent the Extensible Authentication Protocol (EAP) [15] type used to authenticate the dial-up user. It MAY be included in Accounting-Request packets.

A summary of the MS-Acct-EAP-Type Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           EAP-Type
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          EAP-Type (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   24 for MS-Acct-EAP-Type

Vendor-Length
   6

Auth-Type
   The EAP-Type field is 4 octets in length. The following values are currently defined for this field:

MD5	4
OTP	5
Generic Token Card	6
TLS	13

2.7.6. MS-Primary-DNS-Server

Description

The MS-Primary-DNS-Server Attribute is used to indicate the address of the primary Domain Name Server (DNS) [16, 17] server to be used by the PPP peer. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-Primary-DNS-Server Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           IP-Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        IP-Address (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
28 for MS-Primary-DNS-Server

Vendor-Length
6

IP-Address
The IP-Address field is 4 octets in length. It contains the IP address of the primary DNS server.

2.7.7. MS-Secondary-DNS-Server

Description

The MS-Secondary-DNS-Server Attribute is used to indicate the address of the secondary DNS server to be used by the PPP peer. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-Secondary-DNS-Server Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           IP-Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        IP-Address (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
29 for MS-Secondary-DNS-Server

Vendor-Length
6

IP-Address
The IP-Address field is 4 octets in length. It contains the IP address of the secondary DNS server.

2.7.8. MS-Primary-NBNS-Server

Description

The MS-Primary-NBNS-Server Attribute is used to indicate the address of the primary NetBIOS Name Server (NBNS) [18] server to be used by the PPP peer. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-Primary-MBNS-Server Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |           IP-Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        IP-Address (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
30 for MS-Primary-NBNS-Server

Vendor-Length
6

IP-Address
The IP-Address field is 4 octets in length. It contains the IP address of the primary NBNS server.

2.7.9. MS-Secondary-NBNS-Server

Description

The MS-Secondary-NBNS-Server Attribute is used to indicate the address of the secondary DNS server to be used by the PPP peer. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-Secondary-NBNS-Server Attribute format is given below. The fields are transmitted left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-Type  | Vendor-Length |          IP-Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        IP-Address (cont)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor-Type
   31 for MS-Secondary-NBNS-Server

Vendor-Length
   6

IP-Address
   The IP-Address field is 4 octets in length. It contains the IP address of the secondary NBNS server.

3. Table of Attributes

The following table provides a guide to which of the above attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct-Request	#	Attribute
0-1	0	0	0	0	1	MS-CHAP-Response
0	0	0-1	0	0	2	MS-CHAP-Error
0-1	0	0	0	0	3	MS-CHAP-CPW-1
0-1	0	0	0	0	4	MS-CHAP-CPW-2
0+	0	0	0	0	5	MS-CHAP-LM-Enc-PW
0+	0	0	0	0	6	MS-CHAP-NT-Enc-PW
0	0-1	0	0	0	7	MS-MPPE-Encryption-Policy
0	0-1	0	0	0	8	MS-MPPE-Encryption-Type
0-1	0	0	0	0-1	9	MS-RAS-Vendor
0	0-1	0	0	0-1	10	MS-CHAP-Domain
0-1	0	0	0-1	0	11	MS-CHAP-Challenge
0	0-1	0	0	0	12	MS-CHAP-MPPE-Keys
0	0-1	0	0	0	13	MS-BAP-Usage
0	0-1	0	0	0	14	MS-Link-Utilization-Threshold
0	0-1	0	0	0	15	MS-Link-Drop-Time-Limit
0	0-1	0	0	0	16	MS-MPPE-Send-Key
0	0-1	0	0	0	17	MS-MPPE-Recv-Key
0-1	0	0	0	0-1	18	MS-RAS-Version
0-1	0	0	0	0	19	MS-Old-ARAP-Password
0-1	0	0	0	0	20	MS-New-ARAP-Password
0	0	0	0-1	0	21	MS-ARAP-PW-Change-Reason

0	0+	0	0	0+	22 MS-Filter
0	0	0	0	0-1	23 MS-Acct-Auth-Type
0	0	0	0	0-1	24 MS-Acct-EAP-Type
0-1	0	0	0	0	25 MS-CHAP2-Response
0	0-1	0	0	0	26 MS-CHAP2-Success
0-1	0	0	0	0	27 MS-CHAP2-CPW
0	0-1	0	0	0-1	28 MS-Primary-DNS-Server
0	0-1	0	0	0-1	29 MS-Secondary-DNS-Server
0	0-1	0	0	0-1	30 MS-Primary-NBNS-Server
0	0-1	0	0	0-1	31 MS-Secondary-NBNS-Server
0-1	0	0	0	0	33 MS-ARAP-Challenge

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.

4. Security Considerations

MS-CHAP, like PPP CHAP, is susceptible to dictionary attacks. User passwords should be chosen with care, and be of sufficient length to deter easy guessing.

Although the scheme used to protect the Keys field of the MS-CHAP-MPPE-Keys, MS-MPPE-Send-Key and MS-MPPE-Recv-Key Attributes is believed to be relatively secure on the wire, RADIUS proxies will decrypt and re-encrypt the field for forwarding. Therefore, these attributes SHOULD NOT be used on networks where untrusted RADIUS proxies reside.

5. Acknowledgements

Thanks to Carl Rigney (cdr@livingston.com), Ashwin Palekar (ash-winp@microsoft.com), Aydin Edguer (edguer@MorningStar.com), Narendra Gidwani (nareng@microsoft.com), Steve Cobb (stevec@microsoft.com), Pat Calhoun (pcalhoun@eng.sun.com), Dave Mitton (dmitton@baynetworks.com), Paul Funk (paul@funk.com), Gurdeep Singh Pall (gurdeep@microsoft.com), Stephen Bensley (sbens@microsoft.com), and Don Rule (don-aldr@microsoft.com) for useful suggestions and editorial feedback.

6. Editor's Address

Questions about this memo can be directed to:

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Phone: +1 425 703 1559
Fax: +1 425 936 7329
EMail: glennz@microsoft.com

7. References

[1] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Access Dial In User Service", RFC 2138, April 1997.

[4] Zorn, G. and S. Cobb, "Microsoft PPP CHAP Extensions", RFC 2433, October 1998.

[5] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[6] Zorn, G. and G. Pall, "Microsoft Point-to-Point Encryption (MPPE) Protocol", Work in Progress.

[7] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[8] RC4 is a proprietary encryption algorithm available under license from RSA Data Security Inc. For licensing information, contact:
RSA Data Security, Inc.
100 Marine Parkway
Redwood City, CA 94065-1031

[9] Pall, G., "Microsoft Point-to-Point Compression (MPPC) Protocol", RFC 2118, March 1997.

[10] Rand, D., "The PPP Compression Control Protocol (CCP)", RFC 1962, June 1996.

[11] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[12] Richards, C. and K. Smith, "The PPP Bandwidth Allocation Protocol (BAP) The PPP Bandwidth Allocation Control Protocol (BACP)", RFC 2125, March 1997.

[13] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[14] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", Work in Progress.

[15] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[16] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, USC/ISI, November 1987.

[17] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[18] Auerbach, K., and A. Aggarwal, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport", STD 19, RFCs 1001 and 1002, March 1987.

10. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.